

The German Anti-Botnet Advisory Center

Thorsten Kraft

Senior Technical Project Manager
eco – Association of the German Internet Industry

Why an Anti-Botnet Advisory Center?

- There are several million computers worldwide that are part of a Botnetwork – unnoticed by computer owners
- Germany ranked within the Top Ten
- Botnets compose an infrastructure for organized Internet crime

Which dangers are involved within Botnets?

- Distribution of Spam
- Deployment of malicious software
- Server attacks (DDos-Attack)
- Tapping data (Phishing)

Goals of an Anti-Botnet-Advisory Center

- Support users on the subject of Internet security
- Reduce Botnetworks: Free infected computers from malicious software
- Withdraw cyber criminal foundations
- Get Germany out of the Top10 Ranking of malicious activity

What does the Anti-Botnet Advisory Center do?

- helps remove malicious botnet software from an affected users computer
- work together with Internet-Service-Providers (ISPs) and Anti-Virus Software Vendors
- target group: all users using Windows-Computers

What does the Anti-Botnet Advisory Center do?

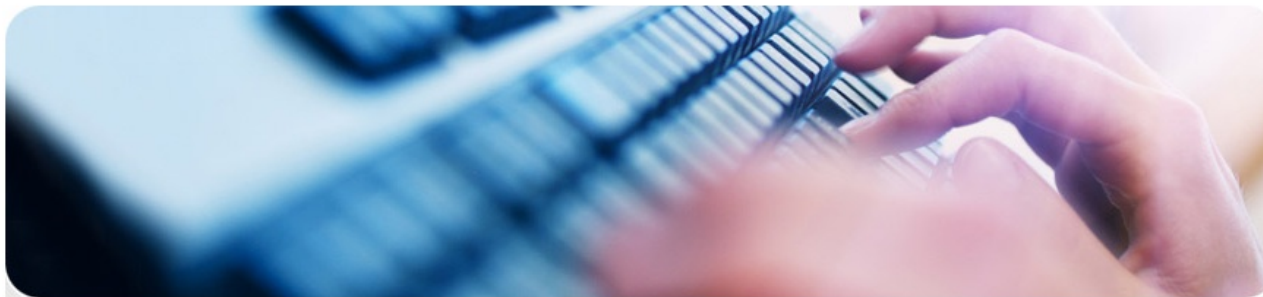
- ISPs/banks detect and notify (various channels) infected customers and refer them to the website of the advisory center
- Call Center module: step-by-step guidance on the phone if necessary
- Ticket System without personal data (Ticket-ID) reports back to ISP/bank

General Framework

- Project setup started March 2010
- Project operation started 15th September 2010
- Start-up funding of up to 2 Million EUR (1,5 Mio spent)
- eco, the association of German ISPs, acts as the exclusive project manager for the initiative
- eco guarantees the continuation for at least another year without additional funding of the government
- BSI provided technical expertise and supports eco
- ISPs take the necessary technical and organisational steps to implement the initiative (informing users, ..)



Bundesamt
für Sicherheit in der
Informationstechnik



Welcome!

[About the Project](#)
[Participants](#)
[Contact](#)
[Data Privacy](#)
[Terms of Use](#)



Welcome to the Anti-Botnet-Advisory Centre, a service from eco – Association of the German Internet Industry with support from the Federal Office for Information Security (BSI).

In the section [Inform](#) find out what Botnets are, what damage they can do and how they can threaten the data on your computer. In the section [Clean](#) our [DE-Cleaner](#) is available. With this tool you'll be able to free your PC from malicious software. In the section [Prevention](#) you will find useful hints on how to protect your computer against re-infection.

“ The Anti-Botnet Initiative is [...] a good example. [...]

This is a good initiative, further will follow. ”

[Former Interior Minister Dr. Thomas de Maizière at the Fifth National IT Summit on the 07.12.2010 in Dresden](#)

Inform → Clean → Prevent

- Internet-Service-Provider (ISP) and/or Bank inform customers of a Botnet infection on his/her computer
- A customer – including all others who are interested too - should visit – www.botfrei.de (available so far in German, English, French, Spanish, Danish, Irish and Turkish language)
- Under *Inform* he/she receives detailed Information about Botnets, Malicious Software and Internet-Security



Clean

• Clean

[DE-Cleaner](#)
[System Rescue CD](#)
[Online Scanner](#)
[Re-installing Windows](#)



We provide a small program which enables you to remove a botnet infection from your computer. The DE-Cleaner will detect and remove malicious files. You will find detailed instructions on how to use this program at the respective menu option.

To prevent re-infection please follow these basic rules:

1. Check whether your computer is infected. Please use our [DE-Cleaner](#). Delete infected files.
2. Install actual service packs and security updates on your system and activate automatic updates [Microsoft Guidelines: Computer Protection](#).
3. Install a Virus Scanner, e.g. one mentioned [here](#) and update it regularly.
4. Use a Firewall e.g. the Windows built-in firewall or a router [More Information about Firewalls](#).

You can find further details about protecting your computer here on our [Prevention](#) page.

Inform → Clean → Prevent

- **DE-Cleaner** detects malicious software and removes it.
- The DE-Cleaner System Recovery-CD can be used for heavily infected computers
- Telephone support hotline help customers needing additional help



Prevention Measures

• Prevention

[Windows Settings](#)
[Private Sector Products](#)
[Enterprise Sector Products](#)
[Firewall](#)



In order to ensure optimal protection, it is necessary that system updates are made on a regular basis and not to forget, automated. In this section we describe how you can protect your system against infection. These measures can help you to surf safer on the Internet.

Regarding the security of your computer, please consider following these basic important rules:

1. Check if your computer has been infected. Please use our [DE-Cleaner](#), and delete infected files.
2. Install current service packs and security updates for your system and activate automatic updates. [Microsoft-Guidelines: Computer Protection](#).
3. Install a Virus Scanner, e.g. one mentioned [here](#) and keep it up-to-date.
4. Use a Firewall e.g. Windows built-in Firewall or a Router. [More Information about Firewalls](#).

Despite using these technical preventions you should however always be suspicious about any email from unknown senders and/or dubious content, such as prize notification, requests, entering your bank account details in webpages, and email attachments.

[continue to "Windows Settings"](#)

Inform → Clean → Prevent

1. **Check** Computers on a regular basis
2. Install actual **Service-Packs and Security Updates** for that operating system including all other application software
3. Installation and regular updates of an efficient **Anti-Virus Scanner**
4. Use a Personal **Firewall** i.e. Windows built-in Firewall or a router Firewall

Partner

ISP participants and others

Customer info

- 1 & 1, GMX & Web.de
- Deutsche Telekom
- Vodafone
- Kabel BW
- Netcologne
- QSC
- Versatel
- Unitymedia
- VZ-Netzwerke

Support hotline

- 1 & 1, GMX & Web.de
- Kabel Baden-Württemberg
- Unitymedia
- VZ-Netzwerke

In short participating Financial Service Providers

signed agreements with / currently being
implemented:

- SSK Solingen
- Naspa
- KSK Köln
- SK Nürnberg
- SK Radevormwald
- KSK Euskirchen

Partner

- DE-Cleaner provided by Avira (since Mar 2011), Kaspersky (Dec 2010) and Norton/Symantec (Sept 2010)
- DE-Cleaner System Rescue CD i.e. Anti-Bot-CD: Avira, BSI, Computerbild and eco

Statistics (15th Sept 10 – 31th Mai 2012)

- **Website Access botfrei.de:**
 - 2,360,606 visitors (10.244.356 page impressions) .
- **blog.botfrei.de** (starting 1st June 11):
 - 4,2561,490 visitors
- **forum.botfrei.de** (starting 1st September 11):
 - 725,623 visitors (support-requests: 29.895)
- **Activations of the provided DE-Cleaners:**
 - 1.391.302** downloads & activations
- Tickets in ticket system = notified end users: **382,493**
 - Less than 2% need telephone support (4549 calls, 2249 email requests)
 - Call duration on average: **10:59** Min.

- **bka-trojaner.de**
 - provides detailed information and instructions on cleaning a bka- & gema-trojan (winlocker/ransomware) infected PCs
 - 613,144 visitors since 29th November 2011
- **dnschanger.eu**
 - WebService with near-live data from Rogue DNS Servers (investigated and overtaken by the FBI/US Gov)
 - Clean: system-dependent guidance
 - 518,662 Visits since 14th December 2011

Statistics: Avira DE-Cleaner Logfile Analysis

Sample month: March 2012:

- scanned Systems: 17,804
- not infected Systems: 10,832
- infected Systems: 6,972
(= **39.16%**)
- Total infected files: 44,251
- infected files per System on average: 8.5

next steps

ACDC will rock over Europe ...
... to fight botnet!

if European Commission agrees ...

next steps

Advanced Cyber Defence Center:

28 partners | 14 member states
8 national support centers

budget: 15,5 million

Detection



report botnet behavior centralized

Centralized Data
Cleaning House



report findings standardized

Notifying
affected
customer



redirect customer to botfree.eu

providing
support



**multi-channel
data collecting:**

honeypot / drone



various sensors



user reports



delivering data

centralized data clearinghouse:

- an approach of collaboration
- different entities working on same data feeds



centralized data
clearing house



standardized data distribution

stakeholder group



output of analyzed data

added values



mitigation



advisories



protection



new tools

receiving data
about infected
customer device



identifying & notifying customer

in BU zu Thorsten

mitigation



pointing to national support center

botfree.eu



Customer self care
- step-by-step
advisories



Individual support:
- call center
- live chat / email
- forum support



Tools:
- disinfection
- to report abuse



Prevention:
- soft- / hardware
- advisories
- warnings

Thorsten Kraft
Senior Technical Project Manager

Lichtstr. 43h
50825 Cologne; Germany

+49 221 / 70 00 48 – 195

thorsten.kraft@eco.de

www.eco.de

www.botfrei.de